Тема: «Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предупреждения»

Информационно-правовые нормы регулируют обособленную группу общественных отношений применительно к особенностям информационной сферы; задает содержание прав и обязанностей субъектов, участвующих в правоотношении.

Информационно-правовые нормы регулируют взаимоотношения граждан, СМИ, организаций, фирм между собой, их взаимные права и обязанности.

Информационная безопасность РФ – состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Права и обязанности участников информационных отношений

- право на защиту личности от воздействия недостоверной, ложной информации;

- право на защиту информации, информационных ресурсов, продуктов от несанкционированного доступа;

- право на защиту интеллектуальной собственности;

- право на защиту информационных систем, информационных технологий и средств их обеспечения как вещной собственности;

- право на защиту информационных прав и свобод;

- ограничение права на раскрытие личной тайны, а также иной информации ограниченного доступа без санкции ее собственника или владельца;

- обязанность по защите государства и общества от вредного воздействия информации, защите самой информации, по защите прав личности, по защите тайны;

- ответственность за нарушение информационной безопасности, в том числе прав и свобод личности, тайны и других ограничений доступа к информации, за компьютерные преступления

Правовое регулирование информационной сферы Российской Федерации

Закон «О правовой охране программ для ЭВМ и баз данных» регламентирует юридические вопросы, связанные с авторскими правами на программные продукты и базы данных.

Закон «Об информации, информатизации и защите информации» позволяет защищать информационные ресурсы (личные и общественные) от искажения, порчи, уничтожения.

В ***Уголовном кодексе РФ*** имеется раздел «Преступления в сфере компьютерной информации». Он предусматривает наказания за:

1. Неправомерный доступ к компьютерной информации;
2. Создание, использование и распространение

Значимость безопасности информации

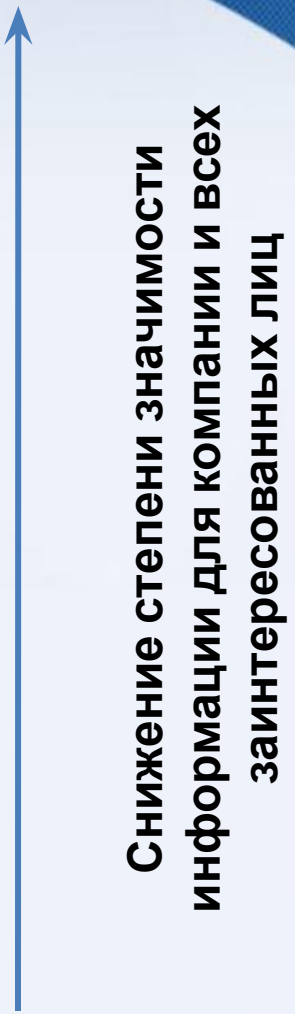
Прикладные задачи: сохранность личной информации пользователя

Управленческие задачи: обеспечение полноты управленческих документов

Информационные услуги: обеспечение доступности и безотказной работы

Коммерческая деятельность: предотвращение утечки информации

Банковская деятельность: обеспечение целостности информации



Методы защиты информации

- Шифрование (криптография) информации
  - Преобразование (кодирование) слов и т.д. с помощью специальных алгоритмов
- Контроль доступа к аппаратуре
  - Вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры
- Законодательные меры
- Ограничение доступа к информации
  - На уровне среды обитания человека: выдача документов, установка сигнализации или системы видеонаблюдения
  - На уровне защиты компьютерных систем: введение паролей для пользователей

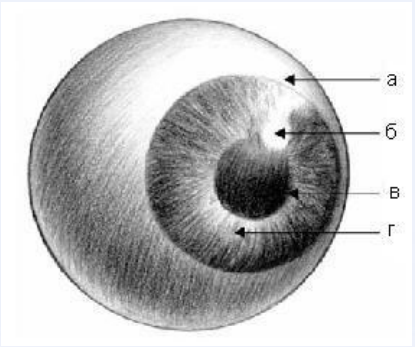
Биометрические системы безопасности – системы контроля доступа, основанные на идентификации человека по биологическим признакам.

Суть биометрических систем сводится к использованию компьютерных систем распознавания личности по уникальному генетическому коду человека. Биометрические системы безопасности позволяют автоматически распознавать человека по его физиологическим или поведенческим характеристикам.

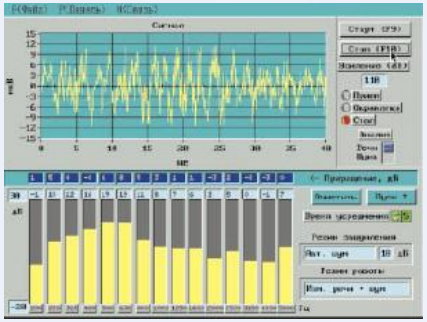
Биометрические системы защиты

По отпечаткам пальцев

По радужной оболочке глаза

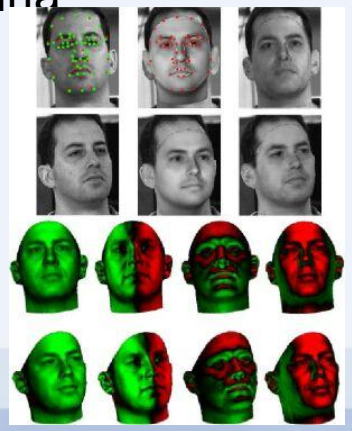


По характеристикам речи



По геометрии ладони руки

По изображению лица




Вредоносные программы
Вирусы, черви, троянские и хакерские программы
Шпионское, рекламное программное обеспечение
Web-черви
Загрузочные вирусы
Почтовые черви
Потенциально опасное программное обеспечение
Файловые вирусы
Троянские утилиты удаленного администрирования
Макровирусы
Троянские программы-шпионы
Рекламные программы
Сетевые атаки
Руткиты
Утилиты взлома удаленных компьютеров
Методы борьбы:
антивирусные программы, межсетевой экран, своевременное обновление системы безопасности операционной системы и приложений, проверка скриптов в браузере